



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/647,676	10/03/2000	Eiji Watanabae	000004.00662	1203

27557 7590 08/27/2004

BLANK ROME LLP  
600 NEW HAMPSHIRE AVENUE, N.W.  
WASHINGTON, DC 20037

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 08/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/647,676

Applicant(s)

WATANABAE ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 03 October 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☒ Claim(s) 4 and 6-8 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 5.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. Claims 1-10 are pending.
2. The references listed on page 12 of the specification have not been considered because they were not listed in an IDS and copies were not provided.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-3, 5, 9-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz, US Patent 5,668,877 in view of Bell, US Patent 6,707,914 further in view of Dole, US Patent 6,628,786 and further in view of Bellare, US Patent 5,491,750.

a) **As to claim 1**, Aziz discloses method and apparatus for stepping pair keys in a key management scheme comprising: an IP key for entering a closed IP network (col. 2, lines 15-20; Fig. 2; col. 6, lines 61-63; col. 8, lines 11-17; lines 44-48); a

key generator for generating from the IP key a set of session keys, which reads on transient key  $K_{sub.p}$ , indexed for identification, the set of session keys having a divergence barrier incorporated therein for barring a computational approach to an arbitrary session key (col. 9, lines 34-42). However, Aziz does not disclose session keys being indexed for identification and having a divergence barrier for barring a computation approach to an arbitrary session key.

Bell teaches the concept of session keys being indexed with index pointer for pointing an index to identify a session key (Figures 5-6).

Aziz and Bell do not disclose session keys having a divergence barrier for barring a computation approach to an arbitrary session key.

Dole discloses a system and method for generating random numbers utilizing a shared or distributed source of entropy, he also discloses an IP key for entering a closed IP network (col. 2, lines 40-46; col. 6, lines 20-24; Fig. 2; col. 8, lines 30-42), he further discloses session keys having a divergence barrier for barring a computation approach to an arbitrary session key (col. 2, lines 53-54, lines 59-67; col. 3, lines 1-2; col. 6, lines 27-35, 50-67; col. 7, lines 5-7; Fig. 1).

Aziz, Bell and Dole do not teach an unbar data set for unbarring the divergence barrier.

Bellare discloses method and apparatus for authenticating communication partners wherein masking and unmasking session key are taught (col. 6, lines 20-24, lines 62-66).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of session keys indexing, session keys having a divergence barrier for barring a computation approach to an arbitrary session key and an unbar data set for unbarring the divergence barrier, as Bell, Dole and Bellare teach, in the system of Aziz so as to easily identify a session key with the index pointer and to achieve additional security by using randomness and masking information.

b) **As to claims 2-3**, Dole discloses the key management mechanism wherein an arbitrary pair of session keys are information-theoretically isolated from each other by a drop of information therebetween having an entropy difference corresponding thereto; and the divergence barrier develops as an integrated entropy difference along a way of the computation approach (col. 3, lines 36-50, 62-67; col. 5, lines 2-10). Dole discloses an integrated entropy difference as divergence barrier, the quantity of entropy in the random number stream is the drop of information between the arbitrary pair of session keys.

c) **As to claim 5**, Dole discloses the key management mechanism wherein the divergence barrier comprises a tree of candidate keys for the arbitrary session key and the tree of candidate keys diverge with an increasing number of candidate keys beyond a computationally secure number, as the computational approach makes a way (col. 5, lines 2-10; col. 7, lines 42-43 to col. 8, lines 1-7, lines 14-25).

d) **As to claim 9**, Dole discloses the key management mechanism wherein the index pointer does not point the index of any session key more than one time (col. 6, lines 3-4).

e) **As to claim 10**, Aziz discloses the key management mechanism wherein part of the unbar data set is built in an outer IP header and transmitted as a cleartext on the closed IP network to a communication peer for a connection less mission of a key agreement in an IP layer of the closed IP network (Fig. 6).

### ***Allowable Subject Matter***

5. Claims 4, 6-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The prior arts of Aziz, Bell, Dole and Bellare do not disclose the claimed key management mechanism wherein the drop of information comprises a lost data on one of a sign data and a numeral data of a respective session key; the unbar data set defines a unique candidate key to be the arbitrary session key; the unbar data set comprises a regenerated set of session keys, which comprising a sequence of boxes of session keys and a respective index combination comprises a combination of a first

index for identifying a unique box of session keys and a second index for identifying the unique session key in the unique box of session keys, and a sequence index combination for identifying a unique session key in the regenerated set of session keys.

### ***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

a) US Patent 5,196,840 to Leith et al. discloses secure communications system for remotely located computers.

b) US Patent 6,708,273 to Ober et al. discloses apparatus and method for implementing IPSEC within an integrated circuit.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 703-306-3036. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Art Unit: 2137

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen  
Examiner  
Art Unit 2137

*mdn*  
mdn  
8/5/04

*Andrew Goldwell*  
Andrew Goldwell